Automatic Secret Keys From Reciprocal MIMO Wireless Channels: Measurement and Analysis

Jon W. Wallace, *Member, IEEE*, and Rajesh K. Sharma, *Student Member, IEEE*

***Abstract*—Information theoretic limits for random key generation in multiple-input multiple-output (MIMO) wireless systems exhibiting a reciprocal channel response are investigated experimentally with a new three-node MIMO measurement campaign. As background, simple expressions are presented for the number of available key bits, as well as the number of bits that are secure from a close eavesdropper. Two methods for generating secret keys are analyzed in the context of MIMO channels and their mismatch rate and efficiency are derived. A new wideband indoor MIMO measurement campaign in the 2.51- to 2.59-GHz band is presented, whose purpose is to study the number of available key bits in both line-of-sight and nonline-of-sight environments. Application of the key generation methods to measured propagation channels indicates key generation rates that can be obtained in practice for four-element arrays.**

***Index Terms*—Cryptography, encryption, measurement, MIMO, time varying channels.**

I. Introduction

SECURE transmission is a concern for wireless devices and networks due to the broadcast nature of signals. The strongest notion of security in the scenario depicted in Fig. 1 is in an information theoretic sense, where Alice and Bob can share information up to the *secrecy capacity*, without providing any information to Eve [1]. Although traditional systems employ private or public-key cryptography separate from physical transmission, there is growing interest in *physical layer security* methods that exploit the propagation channel to strengthen existing cryptosystems.

Developing codes that provide information theoretic security for fading wireless channels is challenging, and automatic secret key generation appears to be more tractable [2]. In [3] and [4], it was proven that matching secret keys can be generated by Alice and Bob by exploiting knowledge of the physical channel and public discussion over an error-free channel. These foundation papers consider two basic models for key generation. In the *source model*, Alice and Bob observe a random process that is observed differently by Eve, and key generation is possible by reconciling errors (mismatches) of the observed sequence over a public channel and distilling information unobservable to Eve. In the *channel* or *wiretap model*, the approach is to generate keys by transmitting random information through the channel, followed by a reconciliation and distillation process. In [2], a practical method for generating secret keys based on the wiretap model is developed, but a drawback of the approach is that Alice and Bob require at least partial channel state information (CSI) of their own channel as well as the eavesdropper channel.

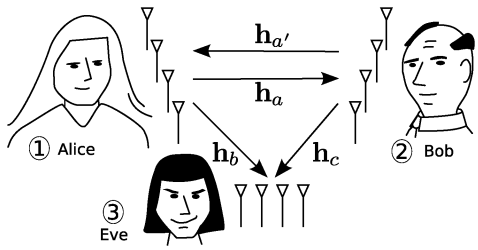

Fig. 1. Wireless communications scenario.

The focus of this paper is systems where the wireless channel is nearly *reciprocal*, opening interesting new possibilities for automatic secret key generation. Practical examples of where reciprocity can be achieved are wireless systems employing time-division duplex (TDD), such as 802.11, 802.16 (WiMAX), and LTE. Reciprocal channel key generation (RCKG) for the source system model, suggested as early as [5], has several attractive features: 1) Since the common random process observed at the two nodes is nearly identical, the key reconciliation process is greatly simplified and reduces to source coding of small mismatches. 2) When the Alice-Bob channel is independent of Eve's channel, perfect secrecy is possible without knowing Eve's channel quality, thus simplifying the secrecy distillation procedure. 3) Alice and Bob never transmit CSI, allowing full channel randomness to be exploited for key generation. 4) Since CSI is passively observed, it can be used in a buffered, off-line fashion, and little modification to existing protocols is required.

Information theoretic aspects of RCKG methods build on the foundation work in secret-key agreement presented in [3] and [4]. More recently, in [6]–[8] an in-depth treatment of secret-key agreement is presented, identifying a nonsimulatability property that indicates whether or not perfectly secure key generation is possible. Further, it is shown that via privacy amplification, a cryptosystem can be made perfectly secure even when Eve has significant information about the shared key. RCKG methods employing quantization are also strongly related to sliced error correction in quantum-distributed Gaussian keys which is treated in [9]. Key generation rates for quantization of scalar Gaussian channels was considered in [10] and applied in

Manuscript received December 17, 2009; revised May 25, 2010; accepted May 25, 2010. Date of publication June 10, 2010; date of current version August 13, 2010. This work was supported by a grant from the German Research Foundation under the COIN Program. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Wade Trappe.

The authors are with the School of Engineering and Science, Jacobs University Bremen, 28759 Bremen, Germany (e-mail: wall@ieee.org; ra.sharma@jacobs-university.de).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2010.2052253

[11] to study channels generated with a path-based propagation model.

Several studies on practical RCKG methods have appeared over the past decade. In [12], the phase of the reciprocal channel is used to randomly rotate the phase of each transmitted data symbol, which is a simple RCKG method with one key symbol per data symbol. The method in [13] exploits reciprocal amplitude fluctuations arising from random switching of parasitic loads. In [14], secret key generation rates for simulated and measured ultrawideband channels are analyzed indicating that high key generation rates can be achieved in practice. In [15], a method is presented based on direct phase quantization for scalar channels. In [16] and [17], a scalar-based quantization method is presented and experimentally verified that exploits amplitude level crossing of the reciprocal channel to robustly generate keys with low mismatch rate. Activity on methods for exploiting common randomness for wireless secret key generation is also apparent in the patent literature (e.g., [18]). Analysis of secure transmission and key agreement techniques for multiple-input multiple-output (MIMO) is also gaining increasing attention [19]–[24], but little work has considered RCKG in a MIMO context.

Although many of the fundamental ideas and limits for RCKG have been developed, to the best of our knowledge, no work has appeared that analyzes the performance of MIMO RCKG in true measured scenarios. Therefore, building on our initial theoretical work in [25] and [26], the primary purpose of this paper is to study limits of RCKG from an experimental perspective, where information theoretic expressions and RCKG protocols are applied to new three-node (for Alice, Bob, and Eve) MIMO measurements taken in an indoor environment in the 2.51- to 2.59-GHz band. Although theoretical results predict N^2 growth of key generation rates for an $N \times N$ MIMO system, our measurements indicate diminishing returns at $N = 4$. Analysis also confirms that most key bits generated with RCKG are secure, even for eavesdroppers with close proximity ($\leq$1 m) and eavesdroppers with an array size or signal-to-noise ratio (SNR) advantage. Finally, the measurements facilitated the development of a realistic RCKG protocol that can be applied to real time-varying MIMO channels. Although seemingly high key generation rates (>30 bits per meter movement) are possible with the protocol, there is significant room for improvement relative to the theoretical limit.

The paper begins in Section II by reviewing the important theoretical results from [26] that are needed to compute and gauge key generation rates for the measured channels. Numerical simulations indicate key generation rates with increasing array size and minimum eavesdropper separation required for high security. Section III presents two practical key generation methods based on channel quantization (CQ) that exploit both amplitude and phase fluctuations for high efficiency and employ guardband or alternating quantization maps to reduce key mismatch rate. Finally, Section IV applies these previous results to measurements from the new MIMO measurement campaign.

II. Limits of Reciprocal Channel Key Generation

This section gives the limits of RCKG for MIMO Gaussian channels. Notational conventions are given in Table I.

TABLE I
Mathematical Notational Conventions

Symbol	Description
x, a, b	Scalars
$\mathbf{x}$, $\mathbf{X}$	Vector and matrix
$\boldsymbol{\mathcal{X}}$	Tensor
$x_{i_1 i_2 \ldots}$	Vector, matrix, or tensor components
$\mathcal{X}$	Discrete or continuous set
N_{qty}	Cardinality (count) of quantity "qty"
$\mathbf{x}^{(n_1,n_2,\ldots)}$	Set of vectors indexed by $(n_1, n_2, \ldots)$
$\hat{\{\cdot\}}$	An estimated quantity (having error)
$\{\cdot\}^*$	Complex conjugate
$\{\cdot\}^T$	Matrix transpose
$\{\cdot\}^H$	Matrix conjugate transpose (Hermitian)
$j = \sqrt{-1}$	Unit imaginary number
$p(X), p(\mathbf{x})$	Probability density function (pdf) of scalar and vector
$\Pr\{\text{event}\}$	The probability of the named event occurring
$g[i, k]$	Function with discrete arguments
$\mathbf{I}$	Identity matrix (size deduced from context)
$h(X)$	Differential entropy of X
$I(X;Y)$	Mutual information of X and Y
$I(X;Y\|Z)$	Conditional mutual information given Z
$\|\mathbf{X}\|$	Determinant of $\mathbf{X}$
$\mathrm{E}\{\cdot\}$	Expectation
$\mathcal{X} \cup \mathcal{Y}$	Union of sets $\mathcal{X}$ and $\mathcal{Y}$
$[a, b]$	The closed interval (continuous set) from a to b
$A \leftarrow B$	The general quantity A is substituted with quantity B

A. System Model

Fig. 1 depicts the model for a wireless communications system. Nodes 1 (Alice) and 2 (Bob) are legitimate users requiring secure communications, while Node 3 (Eve) is a potential eavesdropper. Reciprocal vector channels $\mathbf{h}_a = \mathbf{h}_{a'}$ are referred to as the *forward* and *reverse* channels for legitimate communications, which are estimated by Bob and Alice, respectively. Channels $\mathbf{h}_b$ and $\mathbf{h}_c$ convey information to (and are estimated by) Eve. Note that only passive eavesdroppers are considered in the present work, and considering the robustness of the methods to spoofing attacks is left for future work. Due to noise or synchronization error, the nodes have imperfect estimates of the channels, or

$$\hat{\mathbf{h}}_a = \mathbf{h}_a + \boldsymbol{\epsilon}_2, \quad \hat{\mathbf{h}}_{a'} = \mathbf{h}_{a'} + \boldsymbol{\epsilon}_1, \quad \hat{\mathbf{h}}_b = \mathbf{h}_b + \boldsymbol{\epsilon}_3, \quad \hat{\mathbf{h}}_c = \mathbf{h}_c + \boldsymbol{\epsilon}_3' \tag{1}$$

where $\boldsymbol{\epsilon}_i$ and $\boldsymbol{\epsilon}_i'$ are zero-mean complex Gaussian estimation error at node i having variance σ_i^2. Note that the elements in the channel vectors can be multiple frequency bins for an orthogonal frequency-division-multiplexing (OFDM) system, stacked elements of a MIMO channel, or both.

In the analysis, it is assumed that the channels are zero-mean correlated complex Gaussian random vectors, characterized by the covariance matrices

$$\mathbf{R}_{rp} = E\left\{\mathbf{h}_r \mathbf{h}_p^H\right\} \qquad \hat{\mathbf{R}}_{rp} = E\left\{\hat{\mathbf{h}}_r \hat{\mathbf{h}}_p^H\right\} \tag{2}$$

where $r, p \in \{a, a', b, c\}$. For simplicity, it is assumed that channels are temporally uncorrelated, achievable by sampling the links at intervals longer than the coherence time or prewhitening. Channels with nonzero mean can also be handled by estimating and removing nonfading components.

B. Information Theoretic Limits

For completeness, we include the required results from [26]. The estimated random channels $\hat{\mathbf{h}}_{a'}$ and $\hat{\mathbf{h}}_a$ are observed by

Alice and Bob, respectively, and the maximum number of unique information bits extracted from this process is the mutual information of the observed channels, or $I_K = I(\hat{\mathbf{h}}_a; \hat{\mathbf{h}}_{a'})$. If Eve's channels are dependent on the legitimate channels, she may be able to guess a fraction of the I_K generated bits. The number of secure bits that Alice and Bob can generate is defined as the mutual information of the observed channels given that Eve's channels are known, or $I'_{SK} = I(\hat{\mathbf{h}}_a; \hat{\mathbf{h}}_{a'} | \hat{\mathbf{h}}_b, \hat{\mathbf{h}}_c)$. Since conditioning can possibly increase mutual information, we define $I_{SK} = \min(I'_{SK}, I_K)$, so that $I_{SK} \leq I_K$. The number of vulnerable key bits is defined as $I_{VK} = I_K - I_{SK}$. Note that these definitions are identical to expressions derived and justified in other work. For example, the number of secret bits per observation I_{SK} is identical to the bound defined as $R(X, Y|Z)$ in [14]. The number of available key bits I_K is identical to the quantity $I(X;Y)$ in [10] for a scalar Gaussian channel, which is also the maximum value of I_{SK} when the eavesdropper channels are independent of the channel between Alice and Bob.

Assuming correlated zero-mean complex Gaussian random vectors for the channels

$$I_K = h(\hat{\mathbf{h}}_a) + h(\hat{\mathbf{h}}_{a'}) - h(\hat{\mathbf{h}}_a, \hat{\mathbf{h}}_{a'}) = \log_2 \frac{|\hat{\mathbf{R}}_{aa}||\hat{\mathbf{R}}_{a'a'}|}{|\hat{\mathbf{R}}_{AA'}|}. \quad (3)$$

Here, covariances with lowercase subscripts denote

$$\mathbf{R}_{p_1 p_2} = E\left\{\mathbf{h}_{p_1}\mathbf{h}_{p_2}^H\right\} \quad \hat{\mathbf{R}}_{p_1 p_2} = E\left\{\hat{\mathbf{h}}_{p_1}\hat{\mathbf{h}}_{p_2}^H\right\} \quad (4)$$

while those with uppercase subscripts are covariances of stacked channel vectors, or

$$\mathbf{R}_{P_1 P_2 \ldots P_M} = E\left\{\left[\mathbf{h}_{p_1}^H \mathbf{h}_{p_2}^H \ldots \mathbf{h}_{p_M}^H\right]^H \left[\mathbf{h}_{p_1}^H \mathbf{h}_{p_2}^H \ldots \mathbf{h}_{p_M}^H\right]\right\} \quad (5)$$

with an analogous expression for $\hat{\mathbf{R}}_{P_1 P_2 \ldots P_M}$. For example, covariances in (3) are

$$\hat{\mathbf{R}}_{aa} = \mathbf{R}_{aa} + \sigma_2^2\mathbf{I} \quad \hat{\mathbf{R}}_{a'a'} = \mathbf{R}_{aa} + \sigma_1^2\mathbf{I} \quad (6)$$

$$\hat{\mathbf{R}}_{AA'} = \begin{bmatrix} \mathbf{R}_{aa} + \sigma_2^2\mathbf{I} & \mathbf{R}_{aa} \\ \mathbf{R}_{aa} & \mathbf{R}_{aa} + \sigma_1^2\mathbf{I} \end{bmatrix}. \quad (7)$$

Substituting into (3) and simplifying results in

$$I_K = \log_2 \left|\mathbf{R}_{aa}\mathbf{R}_{\sigma}^{-1} + \mathbf{I}\right| \quad (8)$$

where

$$\mathbf{R}_{\sigma} = \left(\sigma_1^2 + \sigma_2^2\right)\mathbf{I} + \sigma_1^2\sigma_2^2\mathbf{R}_{aa}^{-1}. \quad (9)$$

Note that this result is a generalization of the expression given in [27] for independent identically distributed (i.i.d.) random channels (where $\mathbf{R}_{aa} = \mathbf{I}$).

Evaluation of the secret key bits I_{SK} gives

$$I_{SK} = I(\hat{\mathbf{h}}_a; \hat{\mathbf{h}}_{a'} | \hat{\mathbf{h}}_b, \hat{\mathbf{h}}_c) = \log_2 \frac{|\hat{\mathbf{R}}_{ABC}||\hat{\mathbf{R}}_{A'BC}|}{|\hat{\mathbf{R}}_{BC}||\hat{\mathbf{R}}_{AA'BC}|}. \quad (10)$$

For many practical scenarios, Eve is far away from both Alice and Bob, in which case $\hat{\mathbf{h}}_b$ and $\hat{\mathbf{h}}_c$ are independent of $\hat{\mathbf{h}}_a$ and $\hat{\mathbf{h}}_{a'}$, and I_{SK} becomes (3), meaning all key bits are secure.

We focus on the unfortunate case where Eve is near Alice and Alice and Eve are stationary, leading to correlated channels and reduction in the number of secure key bits. When only movement of Bob or the scatterers causes channel variation, $\mathbf{h}_b$ is not random and contains no information, and (10) is

$$I_{SK} = \log_2 \frac{|\hat{\mathbf{R}}_{AC}||\hat{\mathbf{R}}_{A'C}|}{|\hat{\mathbf{R}}_{C}||\hat{\mathbf{R}}_{AA'C}|}. \quad (11)$$

C. Numerical Examples

An azimuth only single-frequency path-based MIMO channel model [28] is used to simulate a multipath environment connecting Alice and Eve with Bob. Assuming that Eve is near Alice, it is reasonable that they share the same multipath components, and for channel modeling we combine their antennas into one effective array. The complex baseband response connecting Bob's ith antenna with the mth antenna at Alice/Eve is [28]

$$h_{im} = \sum_{\ell=1}^{N_{\text{path}}} \beta_\ell \exp\left[j\left(\mathbf{k}_\ell \cdot \mathbf{x}_i + \mathbf{k}'_\ell \cdot \mathbf{x}'_m\right)\right] \quad (12)$$

where N_{path} is the number of paths, $\mathbf{x}_i = [x_i \; y_i]$ is the 2-D coordinate of Bob's ith antenna in wavelengths, and β_ℓ, $\mathbf{k}_\ell = 2\pi[\cos\phi_\ell \; \sin\phi_\ell]$, and ϕ_ℓ are the complex baseband gain, 2-D wave vector, and angle of the ℓth path, respectively, at Bob. The primed quantities give values with respect to Alice/Eve that are analogous to unprimed quantities for Bob.

Assuming i.i.d. multipath, the full channel covariance is

$$r_{i_1k_1,i_2k_2} = E\left\{h_{i_1k_1}h_{i_2k_2}^*\right\} \quad (13)$$

$$= \sum_{\ell=1}^{N_{\text{path}}} E\left\{|\beta_\ell|^2\right\} \exp\left(j2\pi\psi_{i_1k_1,i_2k_2}\right) \quad (14)$$

$$\psi_{i_1k_1,i_2k_2} = (x_{i_1} - x_{i_2})\cos\phi_\ell + (y_{i_1} - y_{i_2})\sin\phi_\ell + \left(x'_{k_1} - x'_{k_2}\right)\cos\phi'_\ell + \left(y'_{k_1} - y'_{k_2}\right)\sin\phi'_\ell \quad (15)$$

where $E\{|\beta_\ell|^2\}$ is the average power of the ℓth path. The tensor covariance in (13) can be transformed into the required $\mathbf{R}_{aa}$, $\mathbf{R}_{ac}$, and $\mathbf{R}_{cc}$ matrices by extracting the subset of receive antennas corresponding to either Alice or Eve, respectively, and stacking dimensions indexed by i and k.

Defining antenna ranges as $\mathcal{A} = [1, N_1]$, $\mathcal{B} = [1, N_2]$, $\mathcal{E} = [N_1 + 1, N_1 + N_3]$, where N_1, N_2, and N_3 are the number of antennas at Alice, Bob, and Eve, respectively, we can express the extraction of the needed covariances

$$\mathbf{R}_{aa} = \text{reshape}\left\{\boldsymbol{\mathcal{R}}(\mathcal{B}, \mathcal{A}, \mathcal{B}, \mathcal{A}), N_2N_1, N_2N_1\right\} \quad (16)$$

$$\mathbf{R}_{ac} = \text{reshape}\left\{\boldsymbol{\mathcal{R}}(\mathcal{B}, \mathcal{A}, \mathcal{B}, \mathcal{E}), N_2N_1, N_2N_3\right\} \quad (17)$$

$$\mathbf{R}_{cc} = \text{reshape}\left\{\boldsymbol{\mathcal{R}}(\mathcal{B}, \mathcal{E}, \mathcal{B}, \mathcal{E}), N_2N_3, N_2N_3\right\} \quad (18)$$

where $\boldsymbol{\mathcal{R}}(\mathcal{D}_1, \mathcal{D}_2, \mathcal{D}_3, \mathcal{D}_4)$ extracts a subtensor from the fourth-order tensor $\boldsymbol{\mathcal{R}}$ by only considering indices for the first through fourth dimensions that are in the sets $\mathcal{D}_1$ through $\mathcal{D}_4$, respectively, and $\mathbf{R} = \text{reshape}(\boldsymbol{\mathcal{R}}, M, N)$ reshapes the tensor $\boldsymbol{\mathcal{R}}$ into an $M \times N$ matrix using column major ordering. In the following simulations, 5000 random covariance matrices were generated,

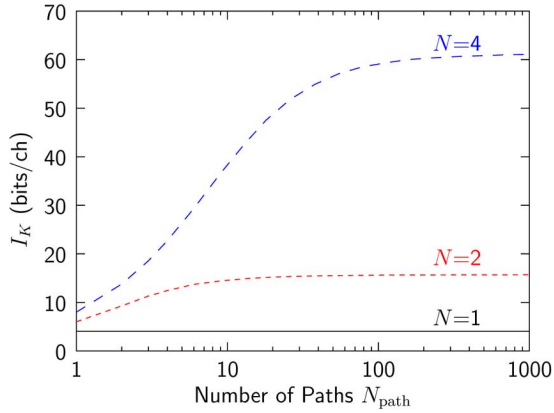

Fig. 2. Theoretical key bits that can be generated for N-element arrays at Alice and Bob and different levels of multipath for 15-dB SNR.

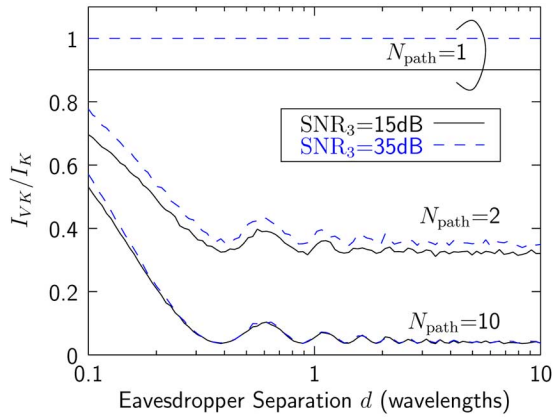

Fig. 3. Relative number of vulnerable key bits for single antenna channels and 15-dB SNR. Eve is distance d from Alice and has either SNR $=$ 15 dB or SNR $=$ 35 dB (advantage).

with path angles uniformly distributed on $[0, 2\pi]$ and path amplitudes equal to $E\{|\beta_\ell|^2\} = 1/N_{\text{path}}$.

Fig. 2 plots I_K versus the number of paths and the number of antennas $N_1 = N_2 = N$ for 15-dB SNR, defined as the mean squared average single-input single-output (SISO) gain to mean squared estimation error. Antennas are ideal vertical dipoles arranged in uniform linear arrays (ULAs) with $\lambda/2$ interelement spacing, where λ is the free-space wavelength. For a fixed number of antennas, the number of available key bits saturates with increasing paths. For rich multipath the increase in I_K goes as N^2 since the channel coefficient for each combination of antennas is an independent random quantity for key generation.

Fig. 3 plots the relative number of vulnerable bits I_{VK}/I_K for a single antenna scenario, where Eve is located a distance d (in wavelengths) from Alice and has either the same SNR as Alice and Bob (15 dB) or a higher SNR (35 dB). Eavesdropper separation below 10λ ($\approx$2 m at 2.55 GHz) is considered since this may be possible for some applications like wireless sensor networks or when a "bug" can be placed in close proximity to a node. Note that the curves are virtually flat for separations above 10λ. Although the eavesdropper can obtain most of the key bits for little separation or limited multipath, the key bits are secure for the separation expected for most applications and moderate multipath. Also, the large SNR advantage actually helps Eve very little when sufficient multipath is present.

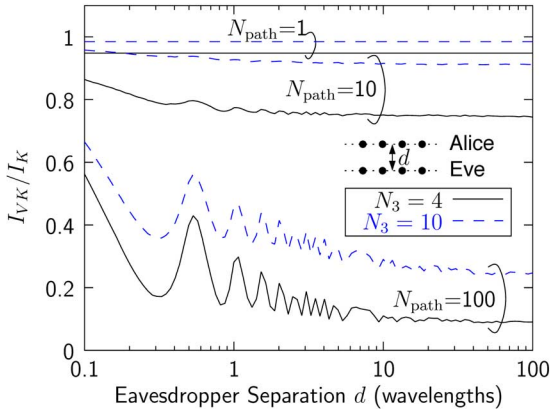

Fig. 4. Relative number of vulnerable key bits for $N = N_1 = N_2 = 4$ antennas and 15-dB SNR, where Eve is distance d from Alice and has either $N_3 = 4$ or $N_3 = 10$ antennas.

Fig. 4 considers a similar scenario with Alice and Bob both having $N = N_1 = N_2 = 4$ antennas, and Eve with either $N_3 = 4$ or $N_3 = 10$ antennas. All nodes employ ULAs, and Alice and Eve's arrays are parallel. Note that not only is richer multipath needed for security, but also eavesdropper separation has a stronger effect for richer channels. The simulation also suggests that eavesdroppers with an array-size advantage are more dangerous to RCKG than those with an SNR advantage. Interestingly, extra vulnerability due to array-size advantage actually increases with additional multipath, which is opposite the behavior seen for SNR advantage.

It is instructive to consider how having additional antennas helps Eve obtain more information about the key. Eve's goal is to estimate $\mathbf{h}_a$ based on observation of $\mathbf{h}_c$, allowing her to generate the same key as Alice and Bob. For a multipath channel, $\mathbf{h}_a$ can be computed from $\mathbf{h}_c$ by estimating path directions and complex amplitudes. For rich multipath, the more antennas at Eve, the more paths she can estimate from $\mathbf{h}_c$ leading to a better possible estimate of $\mathbf{h}_a$.

III. Practical Key Generation Methods

In this section, two key generation methods are developed and analyzed, based on different ways of quantizing the channel information at Alice and Bob. Although it is possible that the quantization method may affect the security of the resulting key, due to space limitations, this will be treated in future work. Here, we assume that Eve's channels are sufficiently independent of the legitimate channels, so that quantization leaks no information about the key bits to Eve. Only scalar channels are considered, but the methods may be applied to multiple parallel channels (MIMO or OFDM) by vectorizing and decorrelating, as shown in Section IV-C.

A. Channel Quantization With Guardband (CQG)

Channel quantization with guardband (CQG) is a generalization of the CQ methods in [15] and [16]. To exploit both amplitude and phase fluctuations, the space of observable complex channels is divided into M equally probable quantization sectors (QSs), where each sector is assigned a unique symbol and corresponding bit pattern. As Alice and Bob observe the

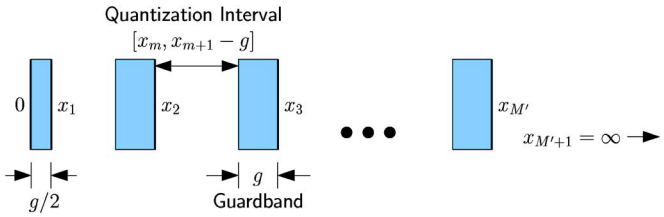

Fig. 5. Parameters for defining one-sided quantization intervals with guardband. Only one positive dimension is required, where x_m is the start of the mth out of M' total quantization intervals separated by guardband g.

channel at specified sample times, the symbols or bits in the corresponding QS are added to the key.

This work assumes rectangular and symmetric QSs (similar to quadrature amplitude modulation (QAM) decision regions), where the problem of defining the QSs is reduced to finding $M' = \sqrt{M}/2$ one-sided (positive axis), one-dimensional quantization *intervals* (QIs), which are then applied separately to real and imaginary parts. The one-sided QIs are defined as depicted in Fig. 5, where guardband g helps avoid mismatch for channel observations near quantization boundaries. An iterative method for finding equal-probability QIs with specified guardband g was given in [26]. Denoting the mth out of M' one-sided quantization intervals as $\mathcal{X}_m^{1s} = [x_m, x_{m+1} - g]$, the complete two-sided set of intervals is

$$\chi_m = \chi_m^{2s} = \begin{cases} -\chi_{M'-m+1}^{1s}, & 1 \le m \le M', \\ \chi_{m-M'}^{1s}, & M'+1 \le m \le 2M' \end{cases} \tag{19}$$

where the 2s superscript is suppressed for simplicity.

Guardband is used to reduce the probability of key symbol mismatch by discarding channels observed in the guardband region. In a one-way handshake, Alice transmits a guardband indicator bit (GIB) to Bob over a public channel, where GIB $= 0$ and GIB $= 1$ indicate observation of the channel outside or inside the guardband, respectively. When GIB $= 1$, both Alice and Bob discard that channel observation. In a two-way handshake, Alice and Bob exchange GIBs and discard the channel if either user declares GIB $= 1$. Increasing guardband gradually reduces the efficiency of key generation, but dramatically reduces the symbol mismatch rate.

To compute the exact efficiency and error probability of CQG, we only need to consider the random real scalars $Y = \mathrm{Re}\{\hat{h}_{a'}\}$ and $Z = \mathrm{Re}\{\hat{h}_a\}$ with variances $\sigma_y^2 = (\sigma_a^2 + \sigma_1^2)/2$ and $\sigma_z^2 = (\sigma_a^2 + \sigma_2^2)/2$, respectively, since the analysis for the imaginary parts is identical. The observation probabilities

$$P_{yz}(\mathcal{Y}, \mathcal{Z}) = \Pr\{Y \in \mathcal{Y} \text{ and } Z \in \mathcal{Z}\} \tag{20}$$

$$P_y(\mathcal{Y}) = \Pr\{Y \in \mathcal{Y}\} \tag{21}$$

$$P_z(\mathcal{Z}) = \Pr\{Z \in \mathcal{Z}\} \tag{22}$$

are required (see Appendix), where $\mathcal{Y}$ and $\mathcal{Z}$ are intervals taken from the QI sets $\mathcal{Y} \in \{\mathcal{Y}_n\}$ and $\mathcal{Z} \in \{\mathcal{Z}_n\}$, for Alice and Bob, respectively.

For the one-way handshake, the one-sided intervals for Alice and Bob are

$$\mathcal{Y}_m^{1s} = [x_m, x_{m+1} - g] \tag{23}$$

and

$$\mathcal{Z}_m^{1s} = [x_m - g/2, x_{m+1} - g/2] \tag{24}$$

respectively. The probability of GIB $= 0$ is

$$P_{\overline{\mathrm{GIB}}} = \sum_{m=1}^{2M'} P_y(\mathcal{Y}_m). \tag{25}$$

Defining observation probabilities conditioned on GIB $= 0$ as $P'_{yz}[m,n] = P_{yz}(\mathcal{Y}_m, \mathcal{Z}_n)/P_{\overline{\mathrm{GIB}}}$, $P'_y[m] = P_y(\mathcal{Y}_m)/P_{\overline{\mathrm{GIB}}}$, and $P'_z[m] = P_z(\mathcal{Z}_m)$, the probability of symbol error for the single real dimension is

$$P'_e = \sum_{m=1}^{2M'} \sum_{\substack{n=1 \\ n \ne m}}^{2M'} P'_{yz}[m,n] \tag{26}$$

and probability of symbol error for the complex case is $P_e = 1 - (1 - P'_e)^2$. We define efficiency of the method as the number of error-free bits obtained per complex channel observation, or

$$\eta = P_{\overline{\mathrm{GIB}}}^2 (1 - P_e) \log_2(M) \tag{27}$$

where a single GIB is used per complex dimension. Of interest is the discrete mutual information after quantization, indicating how much randomness is preserved, which for GIB $= 0$ is

$$I_{K,Q} = \sum_{m=1}^{2M'} \sum_{n=1}^{2M'} P'_{yz}[m,n] \log_2 \frac{P'_{yz}[m,n]}{P'_y[m] P'_z[n]}. \tag{28}$$

For the two-way handshake, $\mathcal{Y}_m$ and $\mathcal{Z}_m$ are both $[x_m, x_{m+1} - g]$, the probability of simultaneous GIB $= 0$ is

$$P_{\overline{\mathrm{GIB}}} = \sum_{m=1}^{2M'} \sum_{n=1}^{2M'} P_{yz}(\mathcal{Y}_m, \mathcal{Z}_n) \tag{29}$$

and expressions for P_e, η, and $I_{K,Q}$ are still given by (26), (27), and (28), respectively.

Note that the method in [16], which we refer to here as channel quantization level crossing (CQLC), is basically equivalent to CQG for a single real dimension with two QIs ($M' = 1$) when positive (q_+) and negative (q_-) CQLC thresholds are $q_+ = -q_- = g/2$. The difference of CQG and CQLC lies in how nonguardband observations are identified and retained. In CQLC, channel observations must belong to an "excursion," which is a run of channel observations of minimum length m that do not fall in the guardband. The nodes then exchange sample indices of excursions in contrast to the single GIB per observation in CQG. The probability of a key symbol mismatch P'_e for CQG with a two-way handshake should be identical to CQLC. Although efficiency of the two methods is basically equivalent for $m = 1$, increasing m may reduce the efficiency of CQLC compared to CQG.

B. Channel Quantization Alternating (CQA)

Instead of using guardband, the error probability can be reduced by simply adapting the quantization map to the channel

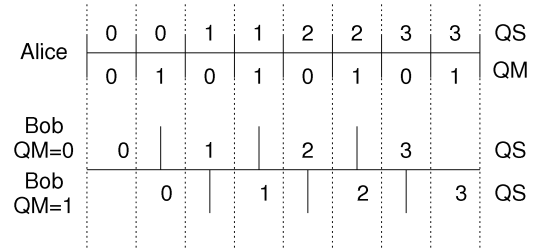

Fig. 6. Example illustrating CQA method for $M' = 2$.

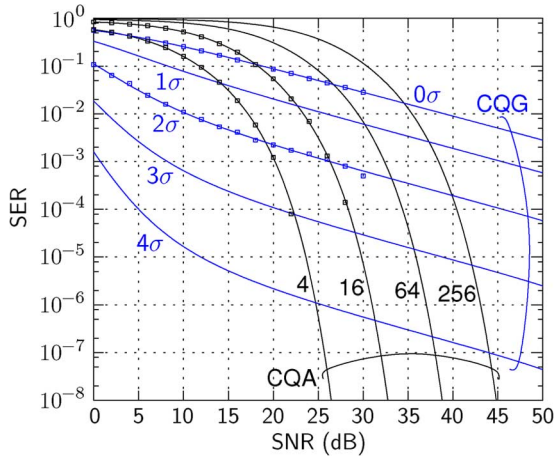

Fig. 7. Exact symbol error rate performance of CQ methods for a single unit variance complex channel with varying guardband g for CQG and varying order M for CQA. Boxes show Monte Carlo simulations.

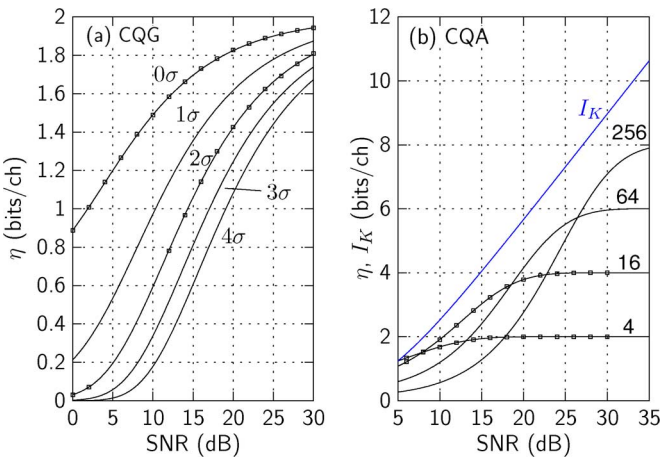

Fig. 8. Exact efficiency η of (a) CQG for different guardband levels g and (b) CQA for different orders M compared with the information theoretic limit I_K. Boxes show Monte Carlo simulations.

observation, which we refer to as channel quantization alternating (CQA), as illustrated in Fig. 6. Before proceeding, we note that CQA is very similar to the coset source coding procedure presented in [29] and adopted in [14]. Also, [17] presents a method termed overquantization that is similar to CQA. In our work, a two-sided set of $4M'$ QIs with equal probability is generated, where each pair of QIs forms a single sector with a given QS index. A quantization map (QM) bit is generated by Alice that indicates which *side* of the sector (or coset) the channel is observed on and transmitted publicly to Bob. Given the QM bit, Bob quantizes his observation of the channel using one of the two alternate maps. Since the QM bit only indicates which side the channel was on, no information about QS is given to Eve. However, the QM bit helps Bob reduce the probability of a symbol error dramatically. Intuitively, for each observed channel, the unused half intervals become guardband for the used interval.

Deriving performance of CQA is similar to CQG. We form a two-sided set of $4M'$ QIs using the methods above with $g = 0$, where the mth raw interval is $\mathcal{W}_m = [w_m, w_{m+1}]$. Alice groups these into left and right pairs or

$$\mathcal{Y}_{L,m} = \mathcal{W}_{2m-1} \tag{30}$$

$$\mathcal{Y}_{R,m} = \mathcal{W}_{2m} \tag{31}$$

and $\mathcal{Y}_m = \mathcal{Y}_{L,m} \cup \mathcal{Y}_{R,m}$. Alice informs Bob that QM $= 0$ if $Y \in \bigcup_{m=1}^{2M'} \mathcal{Y}_{L,m}$, and QM $= 1$, otherwise. Bob's QI map depends on the QM bit, or

$$\begin{aligned} \mathcal{Z}_{L,m} &= [w_{2m-1} - \Delta w_{2m-2}, w_{2m} + \Delta w_{2m}] \\ \mathcal{Z}_{R,m} &= [w_{2m} - \Delta w_{2m-1}, w_{2m+1} + \Delta w_{2m+1}] \end{aligned} \tag{32}$$

where $\mathcal{Z}_m = \mathcal{Z}_{L,m}$ or $\mathcal{Z}_{R,m}$ for QM $= 0$ and 1, respectively, and $\Delta w_m = (w_{m+1} - w_m)/2$. The probability of error is given by (26) with $P'_{yz}[m,n] = P_{yz}(\mathcal{Y}_{L,m}, \mathcal{Z}_{L,n}) + P_{yz}(\mathcal{Y}_{R,m}, \mathcal{Z}_{R,n})$. Discrete mutual information is still given by (28). Since every channel observation is used in CQA, the efficiency is $\eta = (1 - P_e)\log_2(M)$.

C. Numerical Comparison

Fig. 7 plots the uncorrected symbol error rate (SER) performance of the CQ methods for a single complex channel with unit total channel variance and mean square estimation error $\sigma^2 = \sigma_1^2 = \sigma_2^2$. Here, symbol error rate refers to the mismatch rate of key symbols generated by Alice and Bob from observed channels and not symbols transmitted over the channel. For CQG, $M = 4$ and guardband ranges from $g = 0\sigma$ to $g = 4\sigma$, while for CQA, the order M is varied from 4 to 256. Although CQA appears to have much better SER performance at high SNR, this is due to the fact that guardband is defined in terms of σ, which is vanishing with increasing SNR, and for fixed guardband CQG has the same "waterfall" shape as CQA. Also plotted are validating Monte Carlo simulations (10^5 realizations) for a few of the cases.

This plot suggests how to develop an adaptive CQ method, where for a target SER, the CQ type and order M vary with respect to time and the spatial channel as a function of the SNR. Fig. 8 plots the exact efficiency of CQG and CQA. As the order of uncoded CQA is increased with increasing SNR, the efficiency nearly follows the ideal I_K curve. Note that Gray coding and conventional error control could be used to close some of the remaining gap. For CQG, the price paid for low SER is reduced efficiency. Fig. 9 shows the discrete entropy $I_{K,Q}$ of simple CQ (CQG with $g = 0$) and CQA, indicating that CQA usually preserves more of the mutual information I_K, where the maximum gap between CQA and CQG appears to widen with increasing quantization order M.

IV. Application to Measured Indoor MIMO Channels

Although the theoretical results in Section II show that MIMO systems with moderate antennas and SNR ($N = 4$, SNR $=$

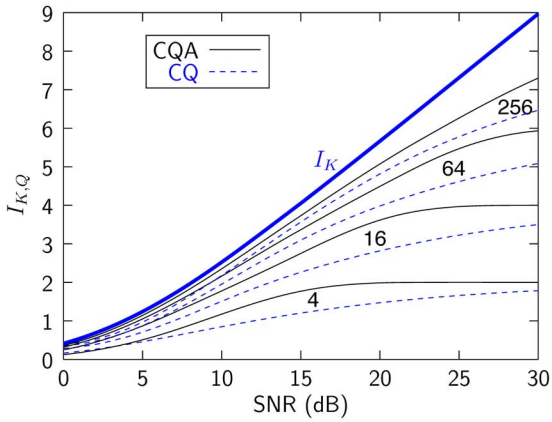

Fig. 9. Discrete mutual information after quantization ($I_{K,Q}$) of simple CQ (CQG with $g = 0$) and CQA for increasing quantization order M.

15 dB) allow key generation rates around 60 bits per channel observation, it is unclear if such rates are supported by true propagation channels. Also, required eavesdropper separation was studied with a very simplistic model where Alice and Eve had a combined array experiencing the exact same multipath directions, perhaps giving a pessimistic view of required separation for secure key generation.

In this section, we present a new indoor MIMO measurement campaign whose purpose was to directly measure available and secure key bits in both line-of-sight (LOS) and nonline-of-sight (NLOS) scenarios, indicating the limit on the rate at which key bits can be generated as well as what eavesdropper separation is required for security. Additionally, the data was used to develop a protocol for actual key generation using CQA, and the resulting key generation rates are presented.

Since our primary interest is to study security limits imposed by physical MIMO propagation channels, our present work does not consider practical system aspects, such as node synchronization and sources of nonreciprocity, which can likely be mitigated by careful system design and calibration. Note that small nonreciprocities due to noise, interference, time offset, and imperfect calibration can be handled using the estimation error already considered. Although our approach is perhaps less comprehensive than testbed campaigns like [16], where an actual real-time RCKG algorithm is implemented, exploring our proposed algorithms with measured MIMO channel data is sufficient for the goals of this present work.

A. Measurement Scenario

MIMO measurements were taken on the first floor of the Research I building on the Jacobs University Bremen Campus in Fig. 10, consisting of classrooms and laboratories. Measurements were performed with a custom MIMO channel sounder fabricated at Jacobs University that is functionally equivalent to the switched architecture in [30], except for two enhancements: 1) Very long sequences of back-to-back channel snapshots can be streamed continuously to disk without interruption using custom FPGA-based A/D with real-time channel estimation. 2) Automatic gain control (AGC) is performed with pure digital control, improving accuracy of channel estimates.

MIMO channels were measured with 23-dBm transmit power using a multitone signal consisting of $N_F = 8$ discrete frequencies with 10-MHz separation and centered at 2.55 GHz. Transmit (TX) and receive (RX) employed monopole arrays with $N_T = 8$ TX and $N_R = 8$ RX elements, equivalent to those in [30]. At TX, the monopoles were attached to a ground plane having a predrilled hexagonal grid of holes, and the antenna positions formed a nearly uniform eight-element circular array (5.7 cm $= 0.47\lambda$ interelement spacing, where λ is the free-space wavelength at 2.55 GHz). In subsequent analysis, only four of the TX elements are usually considered (a semicircle of adjacent elements), simulating Alice and Bob with the same number of antennas. For all data collected in this work, the worst case postprocessing SNR is 20 dB, such that the measurements can be considered virtually error free for scenarios analyzed with higher noise (e.g., 15-dB SNR).

Unlike the usual single-link MIMO measurements, the RX antennas were partitioned into two separate four-element square arrays (5 cm $= 0.43\lambda$ interelement spacing) to represent Alice and Eve, where each subarray consisted of four antennas in a separate 15 cm $\times$ 15-cm ground plane. The subarrays were fixed to a long wooden plank with mounting holes drilled at regular intervals, and Alice-Eve separation distances d of 10 cm, 25 cm, 1 m, and 2 m were investigated. Both TX and RX arrays were approximately 1.6 m off the ground.

TX and RX were placed on carts, where the TX remained stationary throughout the measurement and the RX was pushed along a straight path at approximately 0.3 m/s to obtain a time-varying channel. Given the channel measurement repetition rate of one snapshot per 3 ms, the spatial sampling resolution along the path is 130 snapshots/λ, sufficient to ensure quasi-static channel conditions for a single switched snapshot. For each TX/RX position, eight measurements were taken, consisting of two trials for each of the four different Alice-Eve separations.

The raw channel snapshot for the ith receiver, jth transmitter, fth frequency, and nth temporal sample is denoted $h^{(f,n)}_{\text{raw},ij}$, where $i \in [1,4]$ is Alice, $i \in [5,8]$ is Eve, and j is Bob's antenna index. Channels are normalized so that each $\mathbf{H}^{(f,n)}_{\text{raw}}$ has unit SISO gain [28], which simulates a system with power control and has the added benefit of removing bulk power changes due to deterministic path loss and slow-fading (shadowing). A time series of channel covariances is obtained by dividing temporal snapshots into blocks having $N_B = 1297$ samples each (equivalent to 10λ distance along the path), and computing the full channel covariance for block n

$$r^{(n)}_{ij,k\ell} = \frac{1}{N_B N_F} \sum_{f=1}^{N_F} \sum_{m=(n-1)N_B+1}^{nN_B} h^{(f,m)}_{ij} h^{(f,m)*}_{k\ell}. \quad (33)$$

For LOS scenarios, we apply principal component removal (PCR) to remove effects of the nonfading LOS component. This is accomplished by reshaping the tensor $\boldsymbol{\mathcal{R}}^{(n)}$ in (33) into a matrix, or $\mathbf{R}^{(n)} = \text{reshape}(\boldsymbol{\mathcal{R}}^{(n)}, N_T N_R, N_T N_R)$ and computing the eigenvector $\boldsymbol{\xi}^{(n)}$ that corresponds to the maximum eigenvalue of $\mathbf{R}^{(n)}$. The operation

$$\mathbf{h}^{(f,m)} \leftarrow \mathbf{h}^{(f,m)} - \boldsymbol{\xi}^{(n)} \boldsymbol{\xi}^{(n)H} \mathbf{h}^{(f,m)} \quad (34)$$

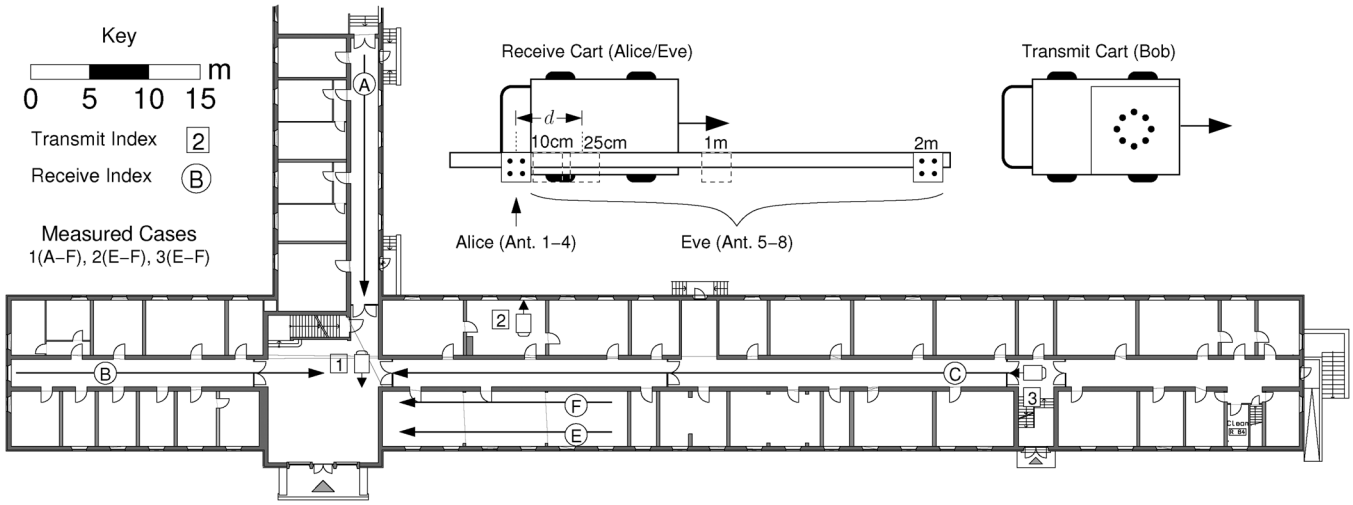

Fig. 10. Indoor measurement scenario on the ground floor of Research I at Jacobs University Bremen. Boxed numbers are stationary transmit (Bob) positions, while circled letters are moving receiver paths (Alice/Eve).

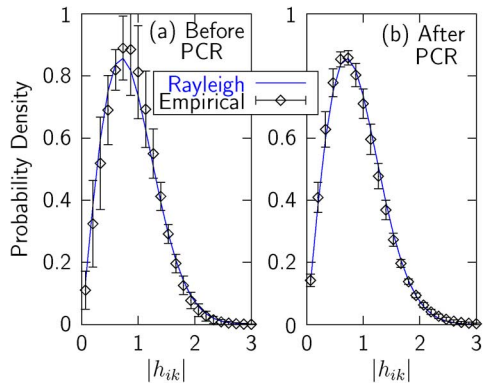

Fig. 11. Marginal pdfs of channel coefficient magnitudes for Location 1C compared to an ideal Rayleigh distribution: (a) before and (b) after applying PCR. Points and error bars indicate the mean and standard deviation of the pdfs computed for the individual blocks.

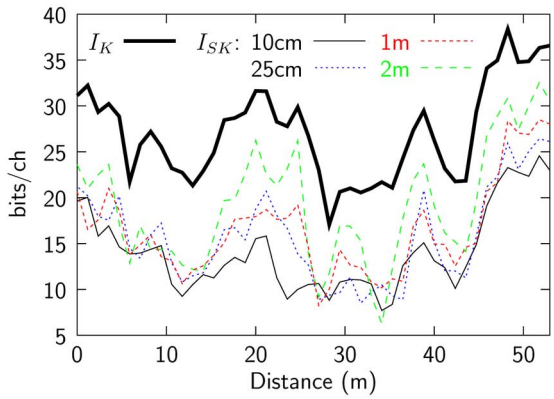

Fig. 12. Available (I_K) and secret (I_{SK}) key bits for LOS Location 1B.

is applied for all channel snapshots m belonging to block n. Fig. 11 plots the marginal empirical probability density function (pdf) of the channel matrix element magnitudes (a) before and (b) after PCR for Location 1C where significant LOS is present, and results for other LOS locations look very similar. Here, individual pdfs are computed for each block, and the mean (points) and standard deviation (error bars) of the pdfs are computed. The results suggest that the data after PCR conforms much better to a Rayleigh distribution than the raw data. Note that the price of PCR is reduced channel power relative to the raw channels.

B. Key Generation Limits of Measured Channels

In this section, we compute the key generation statistics I_K and I_{SK} for measured channels by assuming Gaussian statistics with covariances estimated from measured data using (33). In [17], the issue of deviation of a true fading processes from a Gaussian distribution is raised, which can be a concern when performing security calculations and applying RCKG methods. Our experience in this study is that two main effects can cause non-Gaussian behavior of the channels. First, when nonfading components (such as LOS) are retained, the distribution tends to be more Rician, which can lead to erroneous computations. Second, if the power level changes significantly over a measurement, either due to a changing range or slow-fading (shadowing) effects, the resulting distribution has heavier tails than a Gaussian, which is also problematic. However, as evidenced by Fig. 11, the statistics look nearly Gaussian when the PCR and channel normalization are applied. Also, when the CQ methods are applied in Section IV-C, we show nearly equal frequency of key symbols, suggesting that the data is sufficiently Gaussian for the methods we consider.

Fig. 12 plots I_K and I_{SK} for Location 1B for normalized channels after PCR for assumed SNR of 15 dB. The number of available key bits varies between 20 and 40 bits/ch, around half of the theoretical value for rich multipath channels. Note that the highest I_K occurs at the end of the path, where the receiver transitions from the hallway to an open foyer, which is reasonable since larger angular spread of the multipath would be present. Interestingly, at positions in the hallway with high I_K, values for I_{SK} depend more strongly on eavesdropper separation d, which is similar to results in Fig. 3, where for higher multipath (higher I_K) the number of secure key bits is a stronger function of eavesdropper separation.

Due to space limitations, all scenarios cannot be presented individually. Instead, we present cumulative distribution functions (cdfs) for LOS and/or NLOS scenarios to study the effect of important system parameters on security.

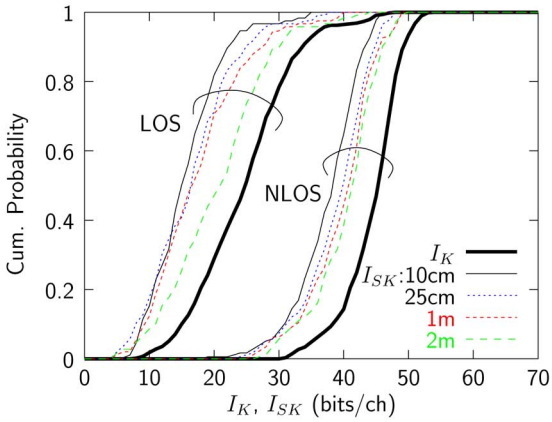

Fig. 13. CDFs for I_K and I_{SK} averaged over all LOS and NLOS scenarios for 15-dB SNR and various eavesdropper separations.

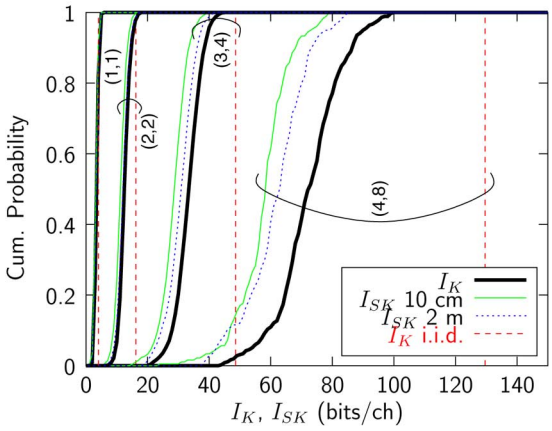

Fig. 14. CDFs for I_K and I_{SK} for NLOS scenarios with varying number of antennas. Curves (N_1, N_2) indicate Alice and Eve have N_1 antennas each and Bob has N_2 antennas.

1) Environmental Effects: LOS versus NLOS: Fig. 13 plots the key generation statistics for I_K and I_{SK} for LOS and NLOS scenarios with $N = 4$ antennas for Alice, Bob, and Eve and SNR $= 15$ dB. LOS channels exhibit about half of the available key bits compared to NLOS, due to the fixed SNR and removal of the high-power LOS component. It is interesting that even for the widest separation of 2 m, there is still a gap of around 4 bits/ch between I_{SK} and I_K. Also clear is that I_{SK} is a weaker function of eavesdropper separation for the NLOS case as compared to LOS.

2) Dependence on Number of Antennas: Fig. 14 plots key generation statistics for varying numbers of antennas for NLOS scenarios only, where curves for (N_1, N_2) indicate N_1 antennas at Alice and Eve and N_2 at Bob. Clearly, for a small number of antennas at Alice and Bob, I_K is near the theoretical maximum for i.i.d. Gaussian channels and most key bits are secure $(I_{SK} \approx I_K)$. However, for increasing numbers of antennas, the gap between ideal I_K and actual I_K as well as the gap between I_K and I_{SK} widen dramatically. A similar trend is also seen for LOS scenarios.

3) Effect of Eavesdropper Advantage: As discussed in the theoretical analysis, an eavesdropper with a significant SNR and/or array size advantage may limit the security of key generation when Eve's channels are correlated with Alice and Bob's

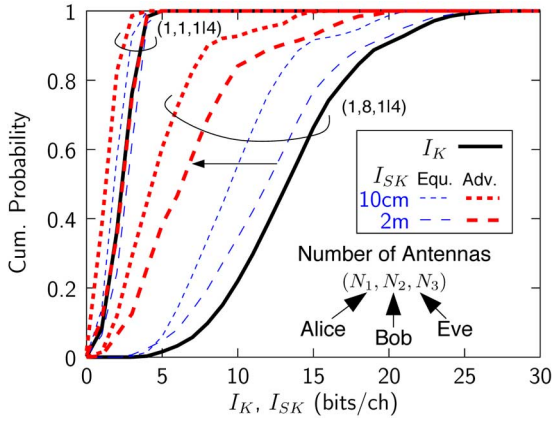

Fig. 15. CDFs of I_K and I_{SK} for LOS scenarios with SNR $= 15$ dB and either 10-cm or 2-m eavesdropper separation. Eve is considered to be equal (Equ.) to Alice $(N_3 = 1)$ or with an antenna $(N_3 = 4)$ and SNR (35 dB) advantage (Adv.).

channels. Fig. 15 depicts statistics for LOS and SNR $= 15$ dB for two extreme cases, where eavesdropper advantage appears to have the minimum and maximum effect. Eavesdropper advantage appears to have little effect for small arrays that are balanced at Alice and Bob ($N_1 = N_2 = 1$ in this case). Note that I_{SK} at 2-m separation is slightly higher than I_K, which occurs because the cdf for I_K includes data for *all* separations, while data for a *specific* separation may have slightly higher or lower I_K and I_{SK} than the average. For the wider eavesdropper separation of 2 m, having an array size $(N_3 = 4)$ and SNR (35 dB) advantage helps Eve negligibly. On the other hand, for unbalanced arrays ($N_1 = 1$, $N_2 = 8$), having more antennas at Eve reduces security significantly, as depicted by the arrow in the figure. Also, we note in general that having an antenna advantage appears to help Eve much more than even a large SNR advantage.

4) Impact of Using Separable Covariances: In real systems with limited CSI, obtaining sufficient channel snapshots to accurately compute the full covariance matrix may not be feasible. In such cases, separate (Kronecker) transmit and receive covariances are more easily computed. A natural question is how much the Kronecker assumption affects the key generation statistics. Specifically, if we compute I_K and I_{SK} based on a Kronecker assumption, how do these values compare with the true I_K and I_{SK} based on the exact full covariance? Fig. 16 plots cdfs of I_K and I_{SK} for LOS and NLOS data computed either with the Kronecker or full covariance. Here, larger eavesdropper separations of 1 and 2 m are used to compute a single cdf of I_{SK}. Although the Kronecker model somewhat overestimates the number of available key bits, perhaps more importantly it suggests that nearly all key bits are secure, when in fact a significant gap is present for the full covariance computations.

C. Simulation of Key Generation on Measured Channels

Theoretical computations indicate between 10 and 60 bits/channel are available for a four-antenna system in the indoor channel. It is of interest to study how many bits can be generated with the CQA method using a practical implementation. Although protocol optimization is a subject of ongoing work, we present a simple adaptive CQA protocol whose performance

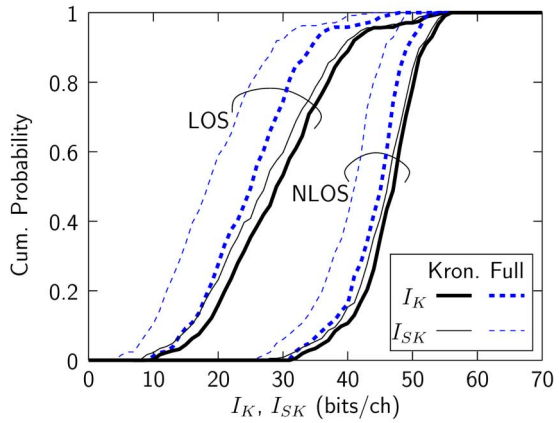

Fig. 16. Comparison of key generation cdfs for LOS and NLOS cases using Kronecker (solid line) or full (dashed line) covariance for 15-dB SNR. Note here that I_{SK} curves use data for both 1- and 2-m separation.

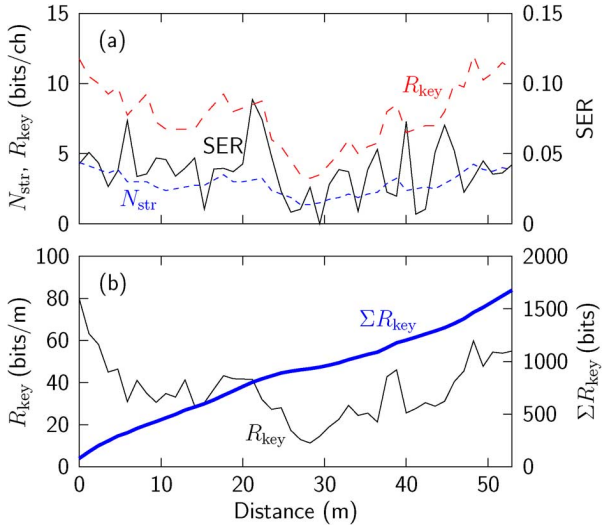

Fig. 17. Key generation statistics with movement for Location 1B for $N_1 = N_2 = 4$ antennas, 15-dB SNR, and maximum target SER 0.1: (a) number of streams ($N_{\rm str}$), SER, key generation rate ($R_{\rm key}$) per channel in each block; (b) key generation rate and accumulated key bits per meter.

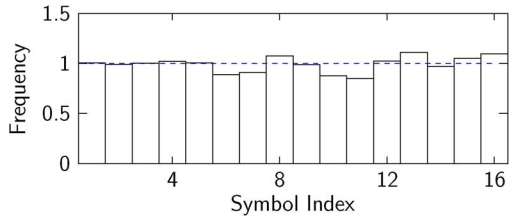

Fig. 18. Ratio of actual to expected frequency of symbols for symbol indices 1–16 for all scenarios.

can be simulated using the measured data. Due to space limitations, we do not consider CQG, which typically has inferior efficiency. The protocol involves the following steps:

1) Subdivide the raw CSI stream into N_B blocks, where each block should be short enough to provide stationary statistics, but long enough to allow estimation of second-order statistics. We employ blocks that are 10λ long.
2) For block m, estimate the temporal channel autocorrelation $\rho^{(m)}[n]$, averaged over the different transmit and receive antennas and frequency bins, where n is sample lag. Fit the autocorrelation to an exponential function $\rho_e^{(m)}[n] = \exp(-\gamma n)$, where the decorrelation sample lag is defined to be $n_d = \lceil 1/\gamma \rceil$.
3) Decimate the CSI samples in block m in time by a factor of n_d in order to obtain nearly independent channel samples. Note that a better strategy combines correlated CSI samples to improve SNR, but since SNR is fixed in our analysis, we use the simple decimation approach.
4) Estimate the spatial covariance using all time and frequency samples.
5) Compute the eigenvalue decomposition (EVD) of the spatial covariance and decorrelate spatial channels by projecting onto the eigenvectors. SNR of the parallel channels can now be computed from the eigenvalues. For LOS, apply PCR by simply discarding the strongest parallel channel.
6) Given a fixed maximum allowed SER, pick the quantization order for each independent channel (e.g., using Fig. 7) that yields the highest symbol rate.
7) Normalize spatial channels to have unit average gain and quantize using precomputed CQA maps. Send a single QM bit from Alice to Bob for each real dimension and each channel observation.
8) Add appropriate symbols and bits to keys.

In a real system, an additional step would be to apply error-control coding sufficient to cover errors up to the target symbol error rate. Also, Step 5 requires the nodes to detect the existence of LOS, which could be accomplished by estimating the Rician K factor and switching modes when a certain threshold is crossed.

Fig. 17 shows key generation statistics for the protocol at LOS Location 1B, assuming four antennas at Alice and Bob, 15-dB SNR, a single frequency bin, and maximum SER of 0.1, and results are averaged over the eight different runs. Fig. 17(a) depicts adaptation of the protocol to changing channel conditions, where the rate $R_{\rm key}$ is the number of key bits generated per independent channel observation, $N_{\rm str}$ is the number of spatial streams in use, and SER is the realized symbol error rate for each block. Fig. 17(b) shows the average key generation rate $R_{\rm key}$ per meter of movement in each block as well as the accumulated key bits for the whole path ($\Sigma R_{\rm key}$). Even for LOS channels, very long keys can be generated or moderate size keys can be renewed frequently. Also note that these results are for a single frequency bin, and exploiting the wideband channel would introduce another multiplication factor.

Fig. 18 gives the number of occurrences of key symbol indices 1–16 divided by the expected number of occurrences for Gaussian channels, where an ideal value is 1.0 (uniform). Although symbol frequency is close to uniform, we note that the frequency of symbols 6, 7, 10, and 11 (innermost quantization sectors for $M = 16$) is slightly low. We have found that this occurs mainly for NLOS cases where the dominant channel is slightly Rician. Better uniformity could be accomplished by using PCR also in NLOS, or by using an adaptive method to dynamically adapt the QSs for the dominant channel. However, the statistics are sufficiently close to Gaussian for the level of quantization considered. Finally, we have observed (not plotted) that the autocorrelation of the key symbol stream is quite low (correlation coefficient below 0.35) in all cases.

TABLE II
AVERAGE KEY GENERATION RATES

	bits/ch		bits/m	
	LOS	NLOS	LOS	NLOS
I_K (all)	22.9	43.9	95.7	302.8
(used)	13.4	29.7	56.7	205.3
Achieved Rate	7.3	16.9	31.1	116.5

Although seemingly high key generation rates are possible with the protocol, there is still a significant performance gap compared to the upper bound I_K. Table II lists the average key generation rates for all LOS and NLOS scenarios as well as I_K, where "all" and "used" indicate I_K for all parallel spatial channels and only those which had sufficient SNR to be used by CQA, respectively. The table indicates ample room for improvement in the algorithm since only 30%–40% of the available I_K is captured.

V. CONCLUSION

This paper has provided an experimental study of key generation methods that exploit reciprocal MIMO channel fluctuations. Simple expressions were presented for the number of available key bits for key generation and the number secure from an eavesdropper. Simulations with a simple multipath channel model indicated that very high key generation rates are possible (60 bits per channel observation for four-element arrays and 15-dB SNR), but that sufficient multipath and eavesdropper separation are needed for most key bits to be secure. Two practical key generation methods were developed and their exact performance computed, indicating that higher efficiency and lower key mismatch rate can be achieved compared to simple direct channel quantization.

A new indoor MIMO measurement campaign for time-varying channels with separate arrays for Alice, Bob, and Eve was conducted to explore theoretical key generation rates and key bit security as well as the performance of the key generation methods in realistic environments. Although the results indicated that the number of available key bits can be significantly lower than the i.i.d. case for larger arrays, the ratio of secure key bits was very similar to the theoretical simulations, where even for close eavesdropper proximity ($\leq$1 m), most key bits are secure. Application of the key generation methods to the measured data indicated that high single-frequency key generation rates (>30 bits/m) with movement are practically achievable, even for LOS scenarios.

APPENDIX

To derive the exact error probabilities of the CQ methods, consider the real zero-mean Gaussian random variables X, ϵ_1, and ϵ_2, with variances σ_x^2, σ_1^2, and σ_2^2, which represent the real or imaginary part of the reciprocal scalar channel and the estimation error at Nodes 1 and 2, respectively. Channel estimates are given by $Y = X + \epsilon_1$ and $Z = X + \epsilon_2$, for the two nodes.

The marginal probability of observing Y on the interval $\mathcal{Y} = [y_1, y_2]$ is obtained by integrating the pdf $p(y) = 1/(\sqrt{2\pi}\sigma_y)\exp[-y/(2\sigma_y^2)]$, where $\sigma_{\{y,z\}}^2 = \sigma_x^2 + \sigma_{\{1,2\}}^2$, or

$$P_y(\mathcal{Y}) = \Pr\{Y \in \mathcal{Y}\} = \frac{1}{2}\left[\operatorname{erf}\left(\frac{y_2}{\sqrt{2}\sigma_y}\right) - \operatorname{erf}\left(\frac{y_1}{\sqrt{2}\sigma_y}\right)\right]. \tag{35}$$

The function for $P_z(\mathcal{Z})$ is identical with $(y, Y, \mathcal{Y}) \leftarrow (z, Z, \mathcal{Z})$. To find the function $P_{yz}(\mathcal{Y}, \mathcal{Z})$, we write the joint pdf of Y and Z as

$$p(y,z) = \frac{1}{2\pi|\mathbf{R}|^{1/2}}\exp\left\{-\frac{1}{2|\mathbf{R}|}S(y,z)\right\} \tag{36}$$

where $S(y,z) = \sigma_x^2(y^2 + z^2 - 2zy) + \sigma_1^2 z^2 + \sigma_2^2 y^2$, and $|\mathbf{R}| = \sigma_x^2(\sigma_1^2 + \sigma_2^2) + \sigma_1^2\sigma_2^2$. The pdf of Z conditioned on Y in a specified interval is

$$\begin{aligned} p(z|Y \in \mathcal{Y}) &= \frac{1}{P_y(\mathcal{Y})}\int_{y_1}^{y_2} p(y,z)dy \\ &= \frac{1}{\sqrt{8\pi}\sigma_z P_y(\mathcal{Y})}\exp\left[-\frac{z^2}{2\sigma_z^2}\right] \\ &\quad \times [A_2(z) - A_1(z)] \end{aligned} \tag{37}$$

where $A_i(z) = \operatorname{erf}[(y_i - \alpha z)\sigma_z/(\sqrt{2}|\mathbf{R}|^{1/2})]$ and $\alpha = \sigma_x^2/\sigma_z^2$. Finally,

$$P_{yz}(\mathcal{Y}, \mathcal{Z}) = \Pr\{Y \in \mathcal{Y}, Z \in \mathcal{Z}\} = \int_{z_1}^{z_2} p(z|Y \in \mathcal{Y})dz \tag{38}$$

which requires two integrals of the form

$$f(z_1, z_2) = \int_{z_1}^{z_2}\exp\left[-\frac{z^2}{2\sigma_z^2}\right]\operatorname{erf}(b - cz)dz. \tag{39}$$

Since the integrand is well behaved, these are computed numerically. In this work, a simple midpoint integration rule was used, and the number of points was chosen to be $N_{\text{int}} = \lceil N_{\text{std}}(z_2 - z_1)/\sigma_z \rceil$, thus giving N_{std} integration points per standard deviation σ_z of the Gaussian kernel. For very large intervals (e.g., z_1 or z_2 infinite) where $z_2 - z_1 > N_{\max}\sigma_z$, and $N_{\max}$ is the maximum number of standard deviations to consider (10 was used in this work), the integration range can be limited without significant loss of accuracy. In this case, we trim the interval to $N_{\max}\sigma_z$ with $z_2 = z_1 + N_{\max}\sigma_z$ when $|z_2| > |z_1|$ or $z_1 = z_2 - N_{\max}\sigma_z$ when $|z_1| \geq |z_2|$.

REFERENCES

[1] J. Massey, "An introduction to contemporary cryptology," *Proc. IEEE*, vol. 76, no. 5, pp. 533–549, May 1988.
[2] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[3] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[4] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography—Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.
[5] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 3–6, Jan. 1995.
[6] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels—Part I: Definitions and a completeness result," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 822–831, Apr. 2003.
[7] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels—Part II: The simulatability condition," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 832–838, Apr. 2003.
[8] U. Maurer and S. Wolf, "Secret-key agreement over unauthenticated public channels—Part III: Privacy amplification," *IEEE Trans. Inf. Theory*, vol. 49, no. 4, pp. 839–851, Apr. 2003.
[9] G. Van Assche, J. Cardinal, and N. J. Cerf, "Reconciliation of a quantum-distributed Gaussian key," *IEEE Trans. Inf. Theory*, vol. 50, no. 2, pp. 394–400, Feb. 2004.
[10] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. 2006 IEEE Intl. Symp. on Information Theory*, Seattle, WA, Jul. 9–14, 2006, pp. 2593–2597.
[11] C. Ye, A. Reznik, G. Sternberg, and Y. Shah, "On the secrecy capabilities of ITU channels," in *Proc. 2007 IEEE 66th Veh. Technol. Conf.*, Baltimore, MD, Sep. 30–Oct. 3 2007.
[12] H. Koorapaty, A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Lett.*, vol. 4, no. 2, pp. 52–55, Feb. 2000.
[13] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.
[14] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.
[15] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. 2008 IEEE Int. Conf. Acoustics, Speech, and Signal Processing*, Las Vegas, NV, Mar. 31–Apr. 4 2008, pp. 3013–3016.
[16] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th ACM Int. Conf. Mobile Computing and Networking (MobiCom'08)*, San Francisco, CA, Sep. 14–19, 2008, pp. 128–139.
[17] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 240–254, Jun. 2010.
[18] I. C. Corporation, "Method and System for Deriving an Encryption Key Using Joint Randomness Not Shared by Others," U.S. Patent Application ITC-2-1135.01.WO, 2006.
[19] A. O. Hero, III, "Secure space-time communication," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.
[20] X. Li and E. P. Ratazzi, "MIMO transmissions with information-theoretic secrecy for secret-key agreement in wireless networks," in *Proc. 2005 IEEE Military Comm. Conf. (MILCOM'05)*, Atlantic City, NJ, Oct. 17–20, 2005, vol. 3, pp. 1353–1359.
[21] X. Zhou, P. Kyritsi, P. Eggers, and F. Fitzek, "The medium is the message: Secure communication via waveform coding in MIMO systems," in *Proc. 2007 IEEE 65th Veh. Technol. Conf.*, Dublin, Ireland, Apr. 22–25, 2007, pp. 491–495.
[22] H. Kim and J. D. Villasenor, "Secure MIMO communications in a system with equal numbers of transmit and receive antennas," *IEEE Commun. Lett.*, vol. 12, no. 5, pp. 386–388, May 2008.
[23] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[24] M. S. Mohammadi, "MIMO minimum leakage-physically secure wireless data transmission," in *Proc. 2009 Int. Conf. Application Information and Communication Technologies*, Baku, Azerbaijan, Oct. 14–16, 2009, pp. 1–5.
[25] J. Wallace, C. Chen, and M. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *Proc. 3rd Eur. Conf. Antennas and Propagation (EuCAP '09)*, Berlin, Germany, Mar. 23–27, 2009, pp. 1499–1503.
[26] J. Wallace, "Secure physical layer key generation schemes: Performance and information theoretic limits," in *Proc. IEEE Int. Conf. Communications (ICC '09)*, Dresden, Germany, Jun. 14–18, 2009, pp. 1–5.
[27] T.-H. Chou, A. M. Sayeed, and S. C. Draper, "Minimum energy per bit for secret key acquisition over multipath wireless channels," in *Proc. 2009 IEEE Int. Symp. Inf. Theory*, Seoul, South Korea, Jun. 28–Jul. 3 2009, pp. 2296–2300.
[28] M. A. Jensen and J. W. Wallace, "A review of antennas and propagation for MIMO wireless communications," *IEEE Trans. Antennas Propag.*, vol. 52, no. 11, pp. 2810–2824, Nov. 2004.
[29] S. S. Pradhan and K. Ramchandran, "Distributed source coding using syndromes (DISCUS): Design and construction," *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 626–643, Mar. 2003.
[30] B. T. Maharaj, J. W. Wallace, M. A. Jensen, and L. P. Linde, "A low-cost open-hardware wideband multiple-input multiple-output (MIMO) wireless channel sounder," *IEEE Trans. Instrum. Meas.*, vol. 57, no. 10, pp. 2283–2289, Oct. 2008.

Jon W. Wallace (S'99–M'03) received the B.S. (summa cum laude) and Ph.D. degrees in electrical engineering from Brigham Young University (BYU) in 1997 and 2002, respectively.

From 1995 to 1997, he worked as an Associate of Novell, Inc. in Provo, UT, and during 1997 he was a Member of Technical Staff for Lucent Technologies, Denver, CO. He worked as a graduate research assistant at BYU until 2002. From 2002 to 2003, he was with the Mobile Communications Group, Vienna University of Technology, Vienna, Austria. From 2003 to 2006, he was a research associate with the BYU Wireless Communications Laboratory. Since 2006, he has been Assistant Professor of Electrical Engineering at Jacobs University, Bremen, Germany. He is also serving as an associate editor of IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION. His current research interests include wireless channel sounding and modeling, wireless security, MIMO communications, cognitive radio, and UWB systems.

Dr. Wallace received the National Science Foundation Graduate Fellowship in 1998.

Rajesh K. Sharma (S'07) received the B.Sc. (with honors) degree in electrical engineering from the University of Engineering and Technology (UET), Lahore, Pakistan, in 1998, and the M.Eng. degree in telecommunications from the Asian Institute of Technology (AIT), Thailand, in 2002. Since 2007, he has studied as a Ph.D. student in the School of Engineering and Science, Jacobs University, Bremen, Germany.

From 1999 to 2001, he worked as a Lecturer and from 2003 to 2007 as an Assistant Professor, both in the Department of Electrical and Electronics Engineering, Kathmandu University, Kathmandu, Nepal. His current research interests include cognitive radio, MIMO communications, wireless physical layer security, and wireless channel modeling.

During his B.Sc. and M.Eng. studies, Mr. Sharma was supported by scholarships from the government of Pakistan and the government of Finland, respectively.